REMARKS

Claims 1 to 15 are pending in the application, with Claim 5 having been amended herein. Claims 1 and 11 to 15 being the independent claims. Reconsideration and further examination are respectfully requested.

As an initial matter, Claim 5 has been amended to correct a typographical error.

The Office Action Summary states that the drawings filed on September 8, 1999 are objected to by the Examiner. However, the Office Action does not set forth any objections to the drawings by the Examiner. Instead, a Form PTO-948 (Notice Of Draftsperson's Patent Drawing Review) is attached to the Office Action which sets forth objections to the original drawings filed on July 20, 1999. Applicants' submit that each of the objections listed on the Form PTO-948 were directed to the original drawings filed on July 20, 1999, and that each listed objection has been corrected in the twelve (12) sheets of formal drawings filed on September 8, 1999. Accordingly, reconsideration and withdrawal of the objections to the drawings are respectfully requested in view of the corrected formal drawings filed in September 8, 1999.

Have Draftsman review it.

The abstract was objected to for various informalities. Applicants submit that the amendments to the abstract set forth herein render moot the foregoing objections. Accordingly, reconsideration and withdrawal of the objections to the abstract are respectfully requested.

OK

Claims 1 to 15 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,793,414 (Shaffer) in view of U.S. Patent No. 6,385,655 (Smith). Reconsideration and withdrawal of the foregoing claim rejections are respectfully requested.

Turning to specific claim language, independent Claim 1 is directed to a method for the secure printing of print data from a client application residing on a data network to a set top box which has a printer, the set top box residing on a digital cable network which has a cable head end for interfacing the digital cable network to the data network. The method includes the steps of generating print data in the client application, determining whether a secure communication path exists between the client application and the set top box, transmitting, in response to a determination that the secure communication path exists, the print data from the client application to the set top box, and sending the print data from the set top box to the printer for printing.

The applied art, namely Shaffer and Smith, is not seen to disclose or suggest the foregoing features of independent Claim 1, particularly with respect to generating print data in the client application residing on a data network, determining whether a secure communication path exists between the client application and the set top box, and transmitting, in response to a determination that the secure communication path exists, the print data from the client application to the set top box.

agree

It is alleged in the Office Action that Shaffer teaches the aforementioned features of independent Claim 1, except for the feature of determining whether a secure communication path exists between the client application and the set top box. Applicants strongly disagree with this assertion. In particular, Shaffer is seen to be directed to an interactive video communication system in which a user of a set-top box can retrieve a high resolution image from a remote data base over a bi-directional communication network, and then print the retrieved high resolution image on a dumb printer connected to the set-top box . (Shaffer, abstract; Fig. 1; column 2, lines 29 to 49; and column 3, lines 10 to 55). However, nowhere is Shaffer seen to disclose or suggest generating print data in a client

agree

application residing on a data network, wherein the client application is separate and distinct from a cable head end for interfacing the digital cable network to the data network..

Instead of generating print data in a client application, Shaffer is simply seen to retrieve a high resolution image from database 22 in the client head end and then to send the rasterized image to set-top box 14. (Shaffer; Fig. 1; and column 3, lines 27 to 55). Unlike the present application, Shaffer is not seen to disclose a data network which is interfaced to the digital cable network through the cable head end, much less a client application on the digital network. In particular, program control computer 16 of Shaffer is connected to set-top box 14 through a digital cable network (bi-directional network 18). (Shaffer; Fig. 1; and column 3, lines 10 to 26). But nowhere is program control computer 16 seen to be connected to another data network besides bi-directional network 18. Accordingly, program control computer 16 cannot be seen to act as an interface between a digital cable network and a data network, as does the cable head end of Claim 1.

In addition, Shaffer is not seen to determine whether a secure communication path exists between the client application and the set top box, and then to transmit, in response to a determination that the secure communication path exists, the print data from the client application to the set top box. Instead, program control computer 16 of Shaffer simply sends the print ready data in blocks to dumb printer 26 via set-top box 14 without making any determination or contingency. (Shaffer; column 3, lines 50 to 55). In contrast, the present invention only transmits the print data from the client application to the set-top box based upon the outcome of a determination. Shaffer is simply not seen to have this ability of optional transmission to the set-top box based on the status of the communication path to the set-top box.

Smith is not seen to remedy the foregoing deficiencies of Shaffer. In particular, Smith is seen to be directed to a method for securely delivering documents over a network which uses special client applications on both the sender and recipient computers. (Smith, abstract; Figure 1; column 2, lines 58 to 67; and column 3, lines 1 to 15). In Smith, the sender computer sends a file to server 22, and then the recipient computer receives a notice, upon which the recipient computer can download the file from server 22. (Smith; column 5, lines 21 to 66). However, nowhere is Smith seen to disclose or suggest that server 22 only transmits the print data to the recipient computer based upon the outcome of a determination of the secure status of the communication path to the recipient computer.

It is alleged in the Office Action that Smith discloses the step of determining whether a secure communication path exists between the client application and the set top box. The portion of Smith relied upon in the Office Action is simply seen to disclose the possibility of using various security methods, such as certificate authentication, for restricting access to the system. (Smith; column 20, lines 41 to 49). However, nowhere is Smith seen to disclose or suggest determining whether a secure communication path exists between a client application on a data network and a set top box on a digital cable network, much less transmitting, in response to a determination that the secure communication path exists, print data from the client application to the set top box.

Based on the foregoing, Applicants respectfully submit that Shaffer and Smith, either alone or in combination, are not seen to anticipate or render obvious the invention of independent Claim 1 because those references are not seen to teach the combination of features in independent Claim 1. Independent Claim 1 is therefore believed to be in condition for allowance, and such action is respectfully requested.

Independent Claim 11 is a method claim containing at least similar features to that of independent Claim 1, in addition to other limitations. As such, independent Claim 11 is also believed to be in condition for allowance for the same reasons discussed above with respect to independent Claim 1.

Independent Claim 12 is directed to a method for the secure printing of print data from a client application residing on a data network to a set top box which has a printer, the set top box residing on a digital cable network which has a cable head end for interfacing the digital cable network to the data network. The method includes generating print data in the client application, transforming, in the client application, the print data from the device-independent format to a rasterized format which corresponds to the printer, encrypting, in the client application, the print data in the rasterized format, sending the encrypted print data in the rasterized format from the client application to the cable head end, sending the encrypted print data in the rasterized format from the cable head end to the set top box, and decrypting, in the set top box, the print data in the rasterized format for printing on the printer.

Shaffer, as discussed above, is not seen anywhere to disclose or suggest the use of encryption and decryption for sending rasterized data from a client application on a data network to a cable head end on a digital cable network, sending the encrypted print data in the rasterized format from the cable head end to the set top box, and then decrypting, in the set top box, the print data in the rasterized format for printing on the printer.

Smith is only seen to disclose the possibility of using various security methods, such as encryption, for restricting access to the system to only authorized users. (Smith; column 20, lines 41 to 49). However, nowhere is Smith seen to disclose or suggest the combination of rasterization, encryption and decryption between a client application,

cable head end and a set-top box as in independent Claim 12. In particular, nowhere is Smith seen to disclose or suggest transforming, in the client application, the print data from the device-independent format to a rasterized format which corresponds to the printer, encrypting, in the client application, the print data in the rasterized format, sending the encrypted print data in the rasterized format from the client application to the cable head end, sending the encrypted print data in the rasterized format from the cable head end to the set top box, and decrypting, in the set top box, the print data in the rasterized format for printing on the printer.

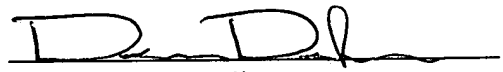
Accordingly, based on the foregoing, independent Claim 12 is also believed to be in condition for allowance. Claims 13, 14 and 15 are directed to apparatus, computer-executable process steps, and computer-readable medium claims, each of which implements the method steps of Claims 1 to 12, and Claims 13, 14 and 15 are therefore also believed to be in condition for allowance.

The other non-allowed claims remaining under consideration in this application are each dependent from the independent claims discussed above and are therefore believed patentable for the same reasons. Because each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration of each on its own merits is respectfully requested.

Based on the foregoing amendments and remarks, the entire application is believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Applicants' undersigned attorney may be reached in our Costa Mesa, CA office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicants

Registration No. 40,595

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 60979 v 1